REMARKS

This Preliminary Amendment is presented to clearly and distinctly claim the invention. No new matter is added. Entry is respectfully requested.

By this amendment, Claims 32-34 have been added. No claims have been amended or cancelled. Hence, Claims 1-34 are pending in the application.

The Examiner is respectfully requested to contact the undersigned by telephone if it is believed that such contact would further the examination of the present application.

To the extent necessary, a petition for an extension of time under 37 C.F.R. § 1.136 is hereby made. Please charge any fee shortages or credit any overages Deposit Account No. 50-1302.

Respectfully submitted,

HICKMAN PALERMO TRUONG & BECKER LLP

Craig G. Holmes
Reg. No. 44,770

1600 Willow Street
San Jose, CA 95125
(408) 414-1080, ext. 207
Date: April 22, 2002
Facsimile: (408) 414-1076

Docket No. 50325-0616 (Seq. No. 4621)

MARKED-UP VERSION OF ALL CLAIMS

All pending claims are reproduced below in marked-up form, whether or not amended, for the convenience of examination.

1   1.   (Not Amended) A method for facilitating Internet security protocol (IPsec) based
2   communications through a device that employs address translation in a
3   telecommunications network, the method comprising the steps of:
4   receiving a first electronic message from a first node, wherein the first electronic
5   message is based on IPsec and is associated with a first identifier;
6   generating a value based on the first identifier;
7   sending the first electronic message to a second node;
8   receiving a second electronic message from the second node, wherein the second
9   electronic message is based on IPsec and is associated with a second
10   identifier that is different than the first identifier, wherein the second
11   identifier is generated based on the first identifier;
12   determining whether the second electronic message is directed to the first node
13   based on the value and the second identifier; and
14   sending the second electronic message to the first node when the second electronic
15   message is determined to be directed to the first node.

1   2.   (Not Amended) A method as recited in claim 1, further comprising the steps of:
2   receiving a third electronic message from a third node, wherein the third electronic
3   message is based on IPsec and is associated with a third identifier;
4   generating an additional value based on the third identifier;
5   sending the third electronic message to the second node;
6   wherein the step of receiving comprises receiving, after sending the first electronic
7   message and the third electronic message to the second node, the second
8   electronic message from the second node, wherein the second electronic
9   message is based on IPsec and is associated with the second identifier that is
10   different than the first identifier and the third identifier;

11   determining whether the second electronic message is directed to the third node

12   based on the additional value and the second identifier; and

13   when the second electronic message is determined to be directed to the third node,

14   sending the second electronic message to the third node.

1   3.   (Not Amended) A method as recited in claim 1, wherein the step of generating the

2   value comprises the step of generating the value based on the first identifier and a

3   specified scheme, and wherein the second identifier is generated based on the first

4   identifier and the specified scheme.

1   4.   (Not Amended) A method as recited in claim 3, wherein the specified scheme

2   produces a fixed length output.

1   5.   (Not Amended) A method as recited in claim 3, wherein the specified scheme is a

2   hash algorithm.

1   6.   (Not Amended) A method as recited in claim 5, wherein the hash algorithm is a

2   Message Digest 5 one-way hash function.

1   7.   (Not Amended) A method as recited in claim 1, wherein the value is a hash value,

2   and wherein the second identifier is the hash value.

1   8.   (Not Amended) A method as recited in claim 1, wherein the value is a hash value,

2   and wherein the second identifier is based at least in part on the hash value.

1   9.   (Not Amended) A method as recited in claim 8, wherein the hash value is comprised

2   of a first plurality of bytes, wherein the second identifier is comprised of a second

3   plurality of bytes, and wherein a last pair of bytes of the second plurality of bytes is a

4   first pair of bytes of the first plurality of bytes, and wherein the step of determining

5   whether the second electronic message is directed to the first node comprises the step

6   of comparing the last pair of bytes of the second identifier to the first pair of bytes of

7   the hash value.

1   10.   (Not Amended) A method as recited in claim 1, wherein the first identifier is a first
2   IPsec security parameter index and the second identifier is a second IPsec security
3   parameter index.

1   11.   (Not Amended) A method as recited in claim 1, wherein the first electronic message
2   is based on IPsec tunnel mode and the second electronic message is based on IPsec
3   tunnel mode.

1   12.   (Not Amended) A method as recited in claim 1, wherein the first electronic message
2   is based on IPsec Encapsulation Security Payload (ESP) and the second electronic
3   message is based on IPsec ESP.

1   13.   (Not Amended) A method as recited in claim 1, wherein the first node is an IPsec
2   originator node and the second node is an IPsec responder node.

1   14.   (Not Amended) A method as recited in claim 1, further comprising the steps of
2   creating and storing a mapping between the value and the first identifier.

1   15.   (Not Amended) A method as recited in claim 14, wherein the step of creating and
2   storing comprises the steps of:
3   creating an association between the value and the first identifier; and
4   storing the association in a translation table.

1   16.   (Not Amended) A method as recited in claim 1, further comprising the steps of:
2   when the second electronic message is determined to be directed to the first node,
3   creating an association between the first identifier and the second identifier;
4   and
5   storing the association in a table.

1   17.   (Not Amended) A method as recited in claim 16, further comprising the steps of:
2   receiving a third electronic message from the second node, wherein the third
3   electronic message is based on IPsec and is associated with the second
4   identifier; and

5   determining that the third electronic message is directed to the first node based on

6   the association.

1   18.   (Not Amended) A method as recited in claim 1, further comprising the steps of:

2   receiving a third electronic from the second node, wherein the third electronic

3   message is based on IPsec and is associated with a third identifier that is

4   different than both the first identifier and the second identifier;

5   determining whether the third electronic message is directed to the first node based

6   on the value and the third identifier; and

7   when the third electronic message is determined to be directed to the first node,

8   sending the third electronic message to the first node.

1   19.   (Not Amended) A method as recited in claim 1, wherein the step of generating the

2   value is performed before the step of receiving the second electronic message.

1   20.   (Not Amended) A method as recited in claim 1, wherein the step of generating the

2   value is performed after the step of receiving the second electronic message.

1   21.   (Not Amended) A method as recited in claim 1, wherein the device employs network

2   address translation (NAT).

1   22.   (Not Amended) A method as recited in claim 1, wherein the device employs dynamic

2   address NAT.

1   23.   (Not Amended) A method as recited in claim 1, wherein the device employs network

2   address port translation (NAPT).

1 24. (Not Amended) A method for facilitating Internet security protocol (IPsec) based

2 communications through a device that employs address translation in a

3 telecommunications network, the method comprising the steps of:

4 receiving a first electronic message from a first node, wherein the first electronic

5 message is based on IPsec and is associated with a first identifier, wherein

6 the first identifier is generated based on a second identifier and the first

7 identifier is different than the second identifier;

8 sending the first electronic message to a second node;

9 receiving a second electronic message from the second node, wherein the second

10 electronic message is based on IPsec and is associated with the second

11 identifier;

12 generating a value based on the second identifier;

13 determining whether the second electronic message is directed to the first node

14 based on the value and the first identifier; and

15 sending the second electronic message to the first node when the second electronic

16 message is determined to be directed to the first node.

1 25. (Not Amended) A method for facilitating Internet security protocol (IPsec) based

2 communications with a device that employs address translation in a

3 telecommunications network, the method comprising the steps of:

4 generating a value based on a first identifier that is associated with a first node;

5 generating a second identifier based on the value;

6 receiving, from the device that employs address translation, a first electronic

7 message that originates from the first node, wherein the first electronic

8 message is based on IPsec and is associated with the first identifier;

9 in response to receiving the first electronic message, generating a second electronic

10 message to the first node, wherein the second electronic message is based on

11 IPsec and is associated with the second identifier;

12 sending the second electronic message to the device that employs address

13 translation;

14   wherein the device determines whether the second electronic message is directed to

15   the first node based on the second identifier and an additional value based on

16   the first identifier; and

17   wherein the device sends the second electronic message to the first node when the

18   device determines that the second electronic message is directed to the first

19   node.

1   26.   (Not Amended) A method as recited in claim 25, wherein the step of generating the

2   second identifier comprises the step of generating the second identifier based on the

3   value and a third identifier.

1   27.   (Not Amended) A method as recited in claim 25, wherein the step of generating the

2   value comprises the step of generating the value based on the first identifier and a

3   specified scheme.

1   28.   (Not Amended) A method as recited in claim 27, wherein the value is a hash value,

2   the first identifier is a first IPsec Security Parameter Index (SPI), the second identifier

3   is a second IPsec SPI, and the step of generating the second IPsec SPI comprises the

4   step of generating, prior to receiving the first electronic message, the second IPsec

5   SPI based on the hash value.

1   29.   (Not Amended) A method as recited in claim 28, wherein the first IPsec SPI is a first

2   randomly generated fixed length value and the step of generating the second IPsec

3   SPI comprises the step of generating the second IPsec SPI based on at least a first

4   portion of the hash value and a second portion of a second randomly generated fixed

5   length value.

1   30.   (Not Amended) A method for facilitating Internet security protocol (IPsec) based

2   communications through a router that employs network address translation in a

3   telecommunications network, the method comprising the steps of:

4   receiving a first electronic message from a first IPsec originator node, wherein the

5   first electronic message is secured using IPsec and is associated with a first

6   security parameter index (SPI);

7	generating a first hash value based on the first SPI and a hash algorithm;
8	sending the first electronic message to an IPsec responder node;
9	receiving a second electronic message from a second IPsec originator node, wherein
10	the second electronic message is secured using IPsec and is associated with a
11	second SPI;
12	generating a second hash value based on the second SPI and the hash algorithm;
13	sending the second electronic message to the IPsec responder node;
14	after sending the first electronic message and the second electronic message to the
15	IPsec responder node, receiving a third electronic message from the IPsec
16	responder node, wherein the third electronic message is secured using IPsec
17	and is associated with a third SPI that is different than the first SPI and the
18	second SPI, wherein the third SPI is generated by the IPsec responder node
19	based at least in part on the hash algorithm;
20	determining whether the third electronic message is directed to the first IPsec
21	originator node based on the first hash value and the third SPI;
22	when the third electronic message is determined to be directed to the first IPsec
23	originator node, sending the third electronic message to the first IPsec
24	originator node;
25	determining whether the third electronic message is directed to the second IPsec
26	originator node based on the second hash value and the third SPI; and
27	when the third electronic message is determined to be directed to the second IPsec
28	originator node, sending the third electronic message to the second IPsec
29	originator node.

1	31.	(Not Amended) A method as recited in claim 30, wherein the first electronic message
2		is based on IPsec tunnel mode and IPsec Encapsulating Security Payload (ESP), the
3		second electronic message is based on IPsec tunnel mode and IPsec ESP, and the
4		hash algorithm is a Message Digest 5 one-way hash function.

1   32.   (New) A computer-readable medium carrying one or more sequences of instructions

2   for facilitating Internet security protocol (IPsec) based communications through a

3   device that employs address translation in a telecommunications network, which

4   instructions, when executed by one or more processors, cause the one or more

5   processors to carry out the steps of:

6   receiving a first electronic message from a first node, wherein the first electronic

7   message is based on IPsec and is associated with a first identifier;

8   generating a value based on the first identifier;

9   sending the first electronic message to a second node;

10   receiving a second electronic message from the second node, wherein the second

11   electronic message is based on IPsec and is associated with a second

12   identifier that is different than the first identifier, wherein the second

13   identifier is generated based on the first identifier;

14   determining whether the second electronic message is directed to the first node

15   based on the value and the second identifier; and

16   sending the second electronic message to the first node when the second electronic

17   message is determined to be directed to the first node.

1   33.   (New) A computer-readable medium carrying one or more sequences of instructions

2   for facilitating Internet security protocol (IPsec) based communications through a

3   device that employs address translation in a telecommunications network, which

4   instructions, when executed by one or more processors, cause the one or more

5   processors to carry out the steps of:

6   receiving a first electronic message from a first node, wherein the first electronic

7   message is based on IPsec and is associated with a first identifier, wherein

8   the first identifier is generated based on a second identifier and the first

9   identifier is different than the second identifier;

10   sending the first electronic message to a second node;

11   receiving a second electronic message from the second node, wherein the second

12   electronic message is based on IPsec and is associated with the second

13   identifier;

14   generating a value based on the second identifier;

15   determining whether the second electronic message is directed to the first node

16   based on the value and the first identifier; and

17   sending the second electronic message to the first node when the second electronic

18   message is determined to be directed to the first node.

1 34. (New) A computer-readable medium carrying one or more sequences of instructions

2   for facilitating Internet security protocol (IPsec) based communications with a device

3   that employs address translation in a telecommunications network, which

4   instructions, when executed by one or more processors, cause the one or more

5   processors to carry out the steps of:

6   generating a value based on a first identifier that is associated with a first node;

7   generating a second identifier based on the value;

8   receiving, from the device that employs address translation, a first electronic

9   message that originates from the first node, wherein the first electronic

10   message is based on IPsec and is associated with the first identifier;

11   in response to receiving the first electronic message, generating a second electronic

12   message to the first node, wherein the second electronic message is based on

13   IPsec and is associated with the second identifier;

14   sending the second electronic message to the device that employs address

15   translation;

16   wherein the device determines whether the second electronic message is directed to

17   the first node based on the second identifier and an additional value based on

18   the first identifier; and

19   wherein the device sends the second electronic message to the first node when the

20   device determines that the second electronic message is directed to the first

21   node.

Docket No. 50325-0616 (Seq. No. 4621)